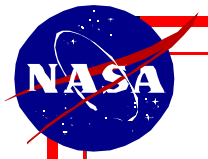


Basic Operation & Management of TCP/IP Networks

ADNET SYSTEMS, Inc.
For the MU-SPIN Coordination Office

Presentation Contents

- *Introduction to the Internet, Protocols and TCP/IP*
- *IP addressing, Name Resolution and DNS*
- *Some of the Protocols described*
- *Network Management using TCP/IP*
- *Serial Line IP (Dial Up)*

Section 1:

Introduction to the Internet, Protocols, and TCP/IP.

Introduction to the Internet and Protocols

Protocol:

- A strictly defined “language” that enables different computers to “talk” (exchange information) across the Internet
- A set of procedures and rules that govern communication
- May be Standard or Proprietary

Standard Protocols:

Protocol specifications are developed by standards committees. Any addition or modification to a protocol must be approved by the appropriate standards committee. Because the specifications are published, many different applications can be developed from different vendors that confirm to the specifications.

- Must conform to the Open System Interconnect (OSI) Reference Model

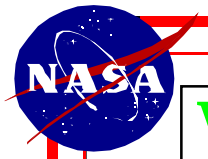
Network Protocols Cont'd.

- Independent from any particular Network type, computer type or Operating System

Proprietary Protocols:

Protocol specifications are developed by private companies. Company holds the right for addition or modification to the protocol. Generally limited to that companies computers and/or Operating System.

- **Novell's IPX (Internet Packet Exchange)**
- **Digital Equipment Corporation's (DEC) DECNet**
- **International Business Machine's (IBM) System Network Architecture (SNA)**
- **Xerox's Xerox Network System (XNS)**



Why Protocols

- **Make communication possible**
- **Reliable exchange of information**
- **Provide a common interface for applications (and users) to exchange information.**
- **Provide independence from and interoperability with the products of different vendors.**

Functions of Protocols

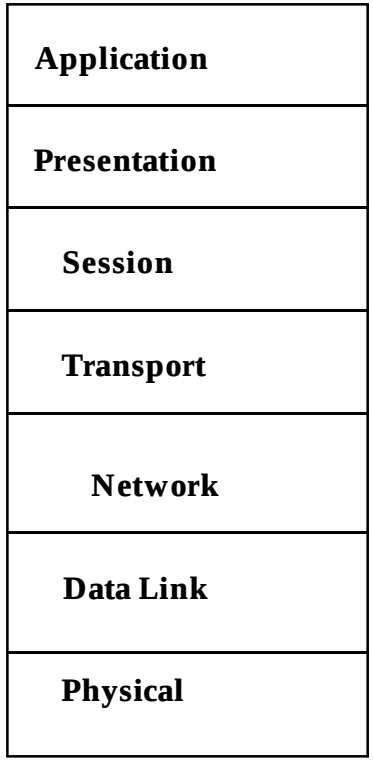
- Provide Network-wide connectivity
- Addressing formats and resolution
- Routing information to its final destination
- Reliable exchange of information
- Segmentation /Fragmentation
- Communication with Network hardware and Computer Operating System
- Controls flow of information between different computer types and network types.

OSI Reference Model

Open System Interconnect Reference Model (OSI - RM)

- A Standard Proposed by the International Standards Organization (ISO).

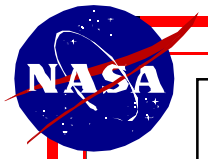
- Performs all functions through the following seven layers:



History of TCP/IP

- Developed in the early 1970's by the Pentagon as a way for military researchers to communicate across the ARPANET, the forerunner of the Internet

- Because the specifications were open, commercial vendors were able to develop applications using the Protocol.



Protocol Layers

The OSI Reference Model defines 7 layers for communications:

Layer 7: Application–a user interface to the network. Includes e-mail applications, web browsers etc.

Layer 6: Presentation–sends/receives data to/from the application in the proper format.

Layer 5: Session–establishes, manages and terminates session connections between applications.

Layer 4: Transport–reliable data transfer, error recovery and flow control.

Protocol Layers

Layer 3: Network–IP addressing and routing of information to final destination.

Layer 2: Data Link–concerned with network hardware addressing, error control and controlling access to the network hardware.

Layer 1: Physical–defines the electrical and mechanical characteristics of the network cabling and interface. For example, ethernet.

TCP/IP Standard Definers

Internet Activities Board (IAB)

Formed in 1983 to guide the evolution of TCP/IP and provide research advice to the Internet community. IAB has formed the following two organizations for technical support:

- **Internet Engineering Task Force (IETF)**

IETF has primary responsibility for further development and standardization of TCP/IP and the integration of other protocols into the Internet. Research organizations, universities, government agencies and computer manufacturers are represented on this body.

- **Internet Research Task Force (IRTF)**

IRTF is mainly involved in internet related basic research

Request For Comments (RFCs)

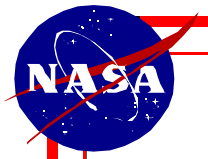
IAB Proposed specification for TCP / IP suites' protocol

Kept on-line at DDN NIC

Can be down-loaded by using anonymous ftp to nic.ddn.mil host. RFC are kept in RFC directory.

List of RFCs for new TCP / IP users

- RFC 1060, "Assigned Numbers"
- RFC 1118, "The Hitchhikers guide to the Internet"
- RFC 1180, "TCP / IP Tutorial"
- RFC 1207, "Answers to Commonly Asked New Internet User Questions"



Section 2:

Internet addressing, Name Resolution and Domain Name Servers.

Internet Addressing

Characteristics

- Each host on the internet has a numeric address, consisting of four fields separated by period. The maximum decimal value for any field is 255, eg 254.123.10.1

- Each address includes a host portion which identifies a host and a network portion which identifies a network

Class

- There are three primary classes: A, B and C

- The Class of address is determined by the first field.

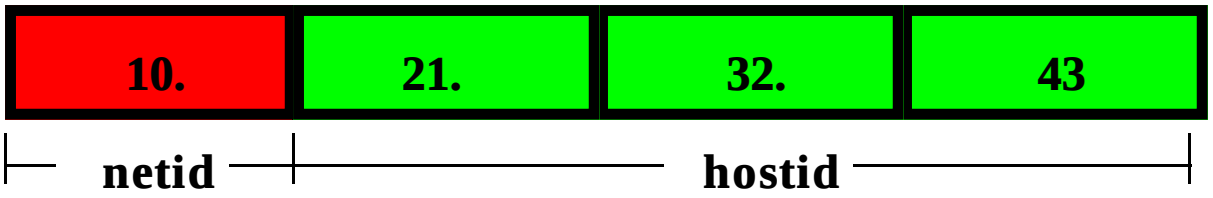
- Class A is for large networks which have more than 65,636 host. For Class A networks, the first field is from 1 to 124, eg 123.10.3.1 is a Class A address.

- Class B is for intermediate networks which have more than 256 hosts but less than 65,636. For Class B networks, the first field is from 128 to 191, eg 128.183.10.23 is a Class B address.

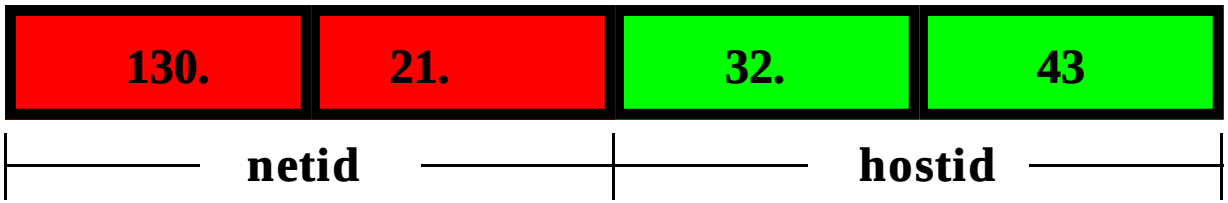
IP Address Ranges

- Class C is for smaller networks that have less than 255 hosts. For a Class C address, the first field is from 192 to 223, eg 198.121.134.10 is a Class C address

Class "A" Addresses

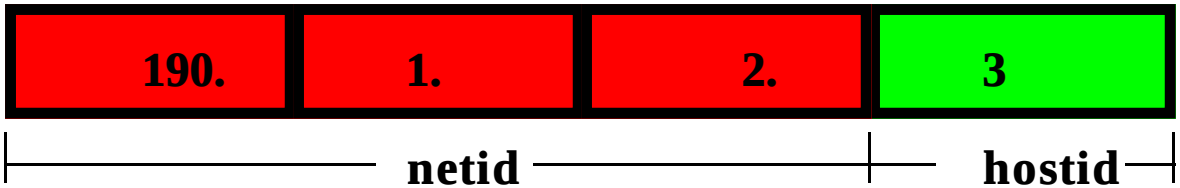


Class "B" Addresses



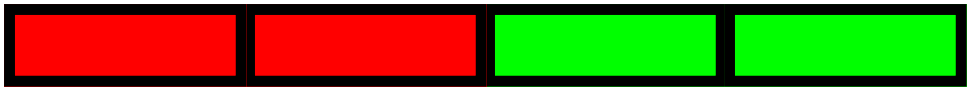
IP Address Ranges

Class "C" Addresses



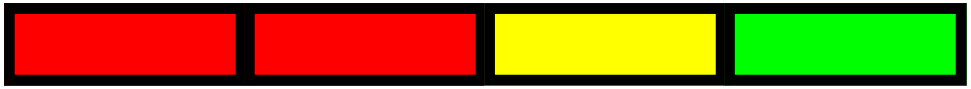
Subnetworking

Scheme to split host part of IP address space into host and subnet parts, in order to make more efficient use of the address space, eg for a Class B address:



Network portion **Host Portion**

A subnetted Class B address could look like this:



Network portion **Subnet Portion** **Host Portion**

Subnetworking

Allows network to be divided into small and independent LANs.

Subnet Mask is needed to route packets between two networks

Easier for management and monitoring

Provides better utilization of IP address space

Transparent to Outside Network

Subnet Masks

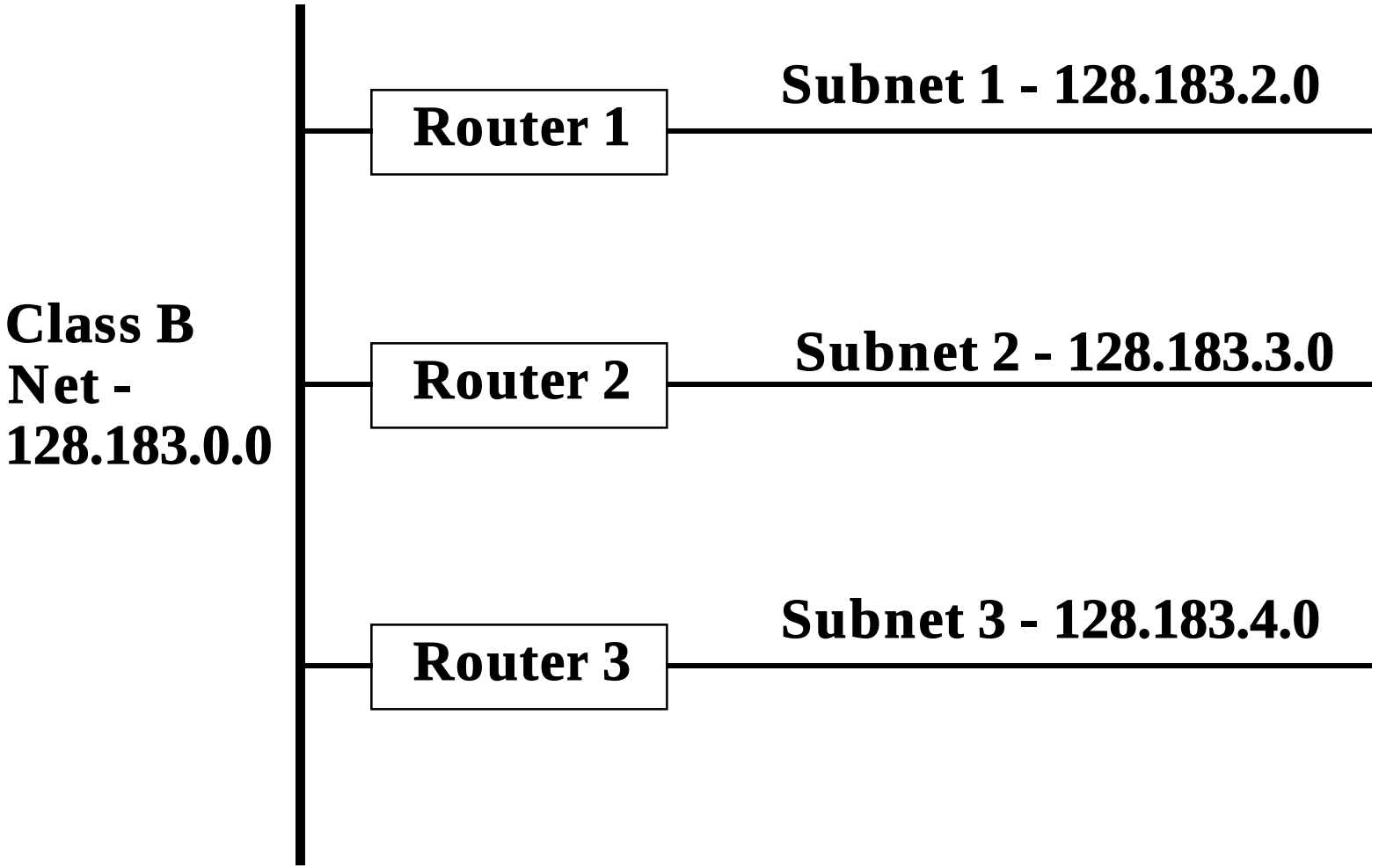
- A subnet mask tells the TCP/IP driver which portion of the IP address is the network portion, and which is the host portion
- Must be manually configured into the TCP/IP setup by user/administrator.

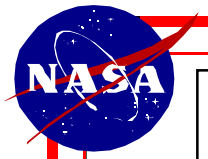
Standard Masks:

- Class A 255.0.0.0
- Class B 255.255.0.0
- Class C 255.255.255.0

When a Class B network is subnetted, the new subnet mask becomes 255.255.255.0

Subnetting Example





IP Name Resolution

Domain Name System

- IP addresses (numbers) are very cumbersome to remember - mistakes are easily made.
- The Internet authorities have come up with a naming system whereby every machine and user can have a name instead of an address
- The system is called DNS and is in a Hierarchical order just like the telephone numbers
- The hierarchy can be geographical or institutional
- DNS specifies two things:

  Name syntax and rules for delegating the authority over names, and a means of resolving domain names into IP addresses

Internet Domain Names

- *Hierarchical* from left to right - more specific domain to the left
- Consist of labels separated by dots muspin.gsfc.nasa.gov
  - .gov is the highest domain
  - .nasa.gov is the second highest domain
  - .gsfc.nasa.gov is the second lowest domain
  - muspin.gsfc.nasa.gov is the lowest domain
- Domain Names are grouped according to activity
  - COM Commercial organizations
  - EDU Educational institutions
  - GOV Government institutes
  - MIL Military
  - NET Network centers
  - ORG Large organizations
  - INT International organizations
  - *country codes* Each country has one

IP Name Resolution

Name Servers

- Domain Name to IP address mapping is accomplished using Name Servers
- Every Domain must have at least 1 and usually 2 Name Servers.
- Name Servers contain entries for every name to IP address map within their zone of authority (usually their domain).
- TCP/IP software contains a module called a Resolver which queries the Name Server for an IP address when required by an application process (such as a Web Browser).
- If the requested address is outside the zone of authority of the local Name Server, it has the address of a Root Server to which the request can be passed for resolution.
- Resolvers and Name Servers maintain a cache of previous lookups to which they refer when a request is received from an application process.

Local Name Resolution

pc1.someu.edu

Student(s)
(clicks on a URL)

Web Browser

Resolver (checks cache first)

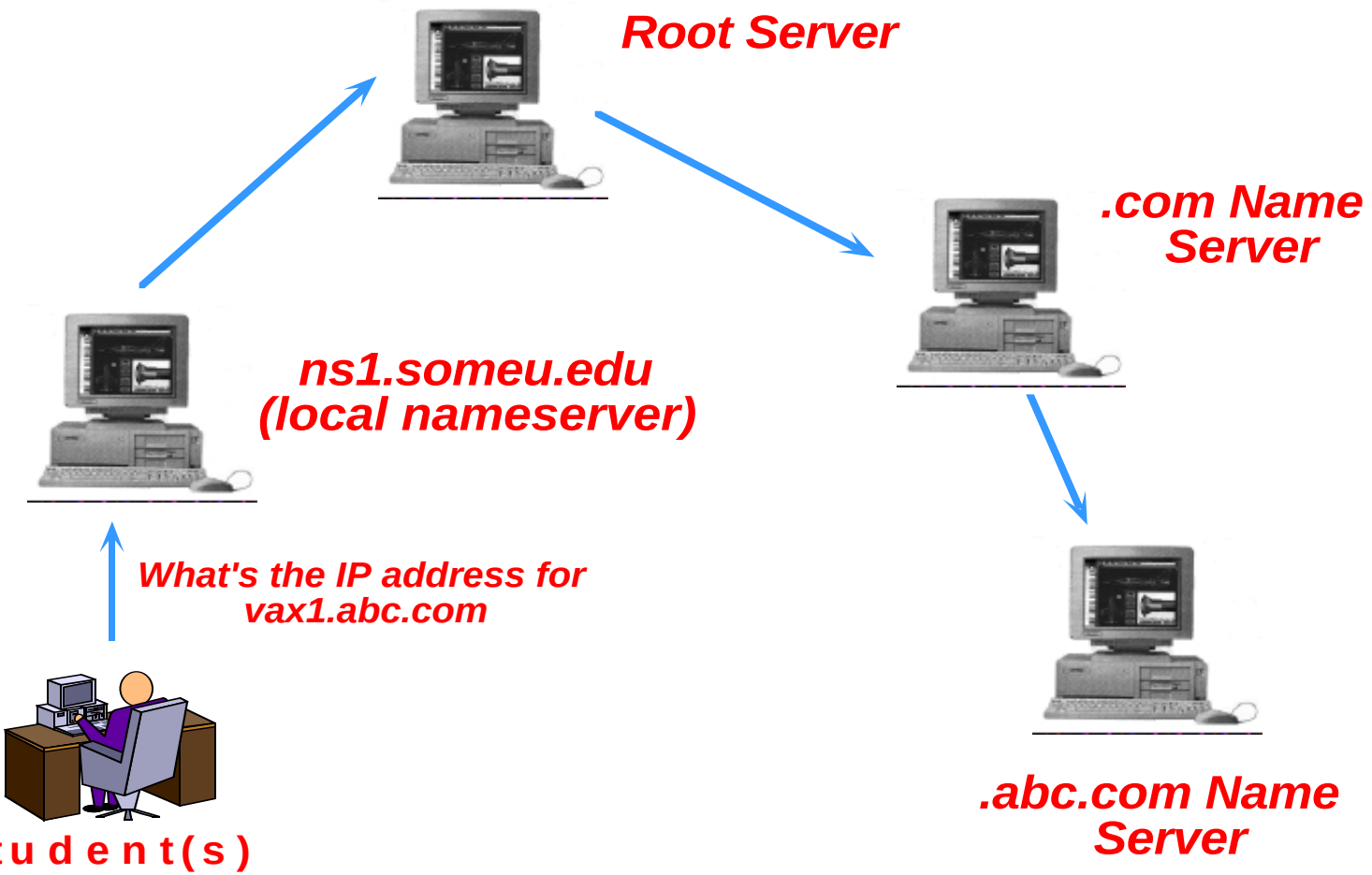
What's the IP address for pc2.someu.edu

ns1.someu.edu
(local nameserver)

Check's cache

The IP address for pc2.someu.edu is 130.123.10.40

Remote Name Resolution

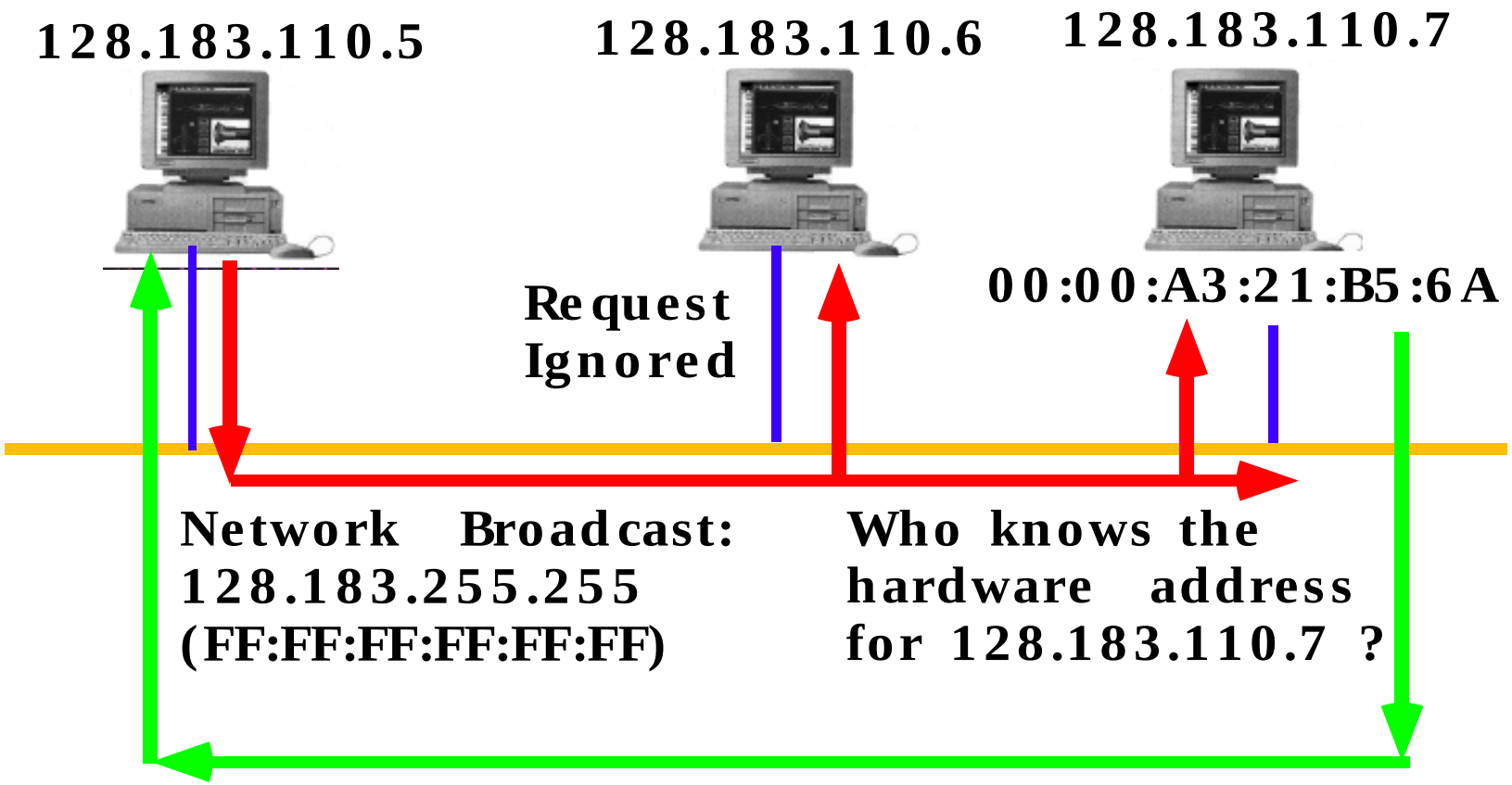


IP Address to Hardware Address Mapping (ARP)

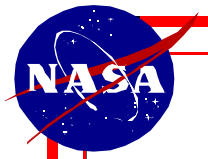
- Provides independence from any particular network hardware
- On local network machines interact with each other by using their respective hardware addresses
- ARP provides dynamic map between IP address and hardware address, usually ethernet address
- Network Broadcast is used to send ARP request
- Hosts maintain in their cache an ARP table (IP addresses of other hosts with their respective hardware addresses)
- Example:

jockey.ubd.edu (555.132.101.32) at 0:0:5a:ef:65:9f

IP Address to Hardware Address Resolution (ARP)



The hardware address for 128.183.110.7 is 00:00:A3:21:B5:6A



Section 3:

Some of the Protocols described

Transmission Control Protocol (TCP)

A reliable, connection oriented Full Duplex (two way) protocol that uses Byte-Stream

Invoked by application layer protocols such as Telnet, FTP and SMTP, or Web Browsers

TCP uses IP to exchange packets between two hosts

Time-outs are used for the Negative Acknowledgments

Urgent data are send by bypassing flow control

Sliding window flow control, end-to-end check and error recovery

IP Operation

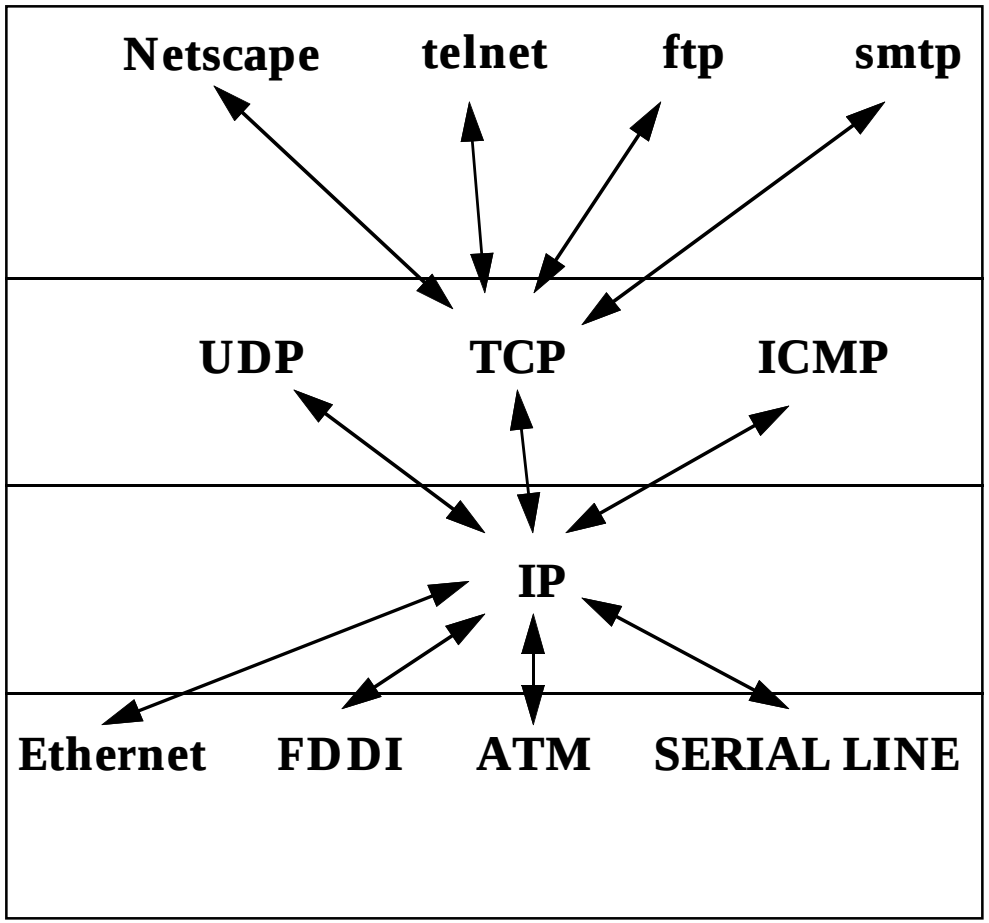
- At the sending host IP, performs the following:

- Construct the datagram
- Perform checksum and append it
- Make routing decision
- Pass datagram to Network Access Protocol (NAP) for X-mission

- Each gateway performs the following

- Checksum
- Decrement Time To Live
- Make routing decision
- Fragmentation if needed
- Rebuild header
- Pass it to the NAP

TCP/IP Layers



application
presentation &
session

transport

network

datalink
and physical

User Datagram Protocol (UDP)

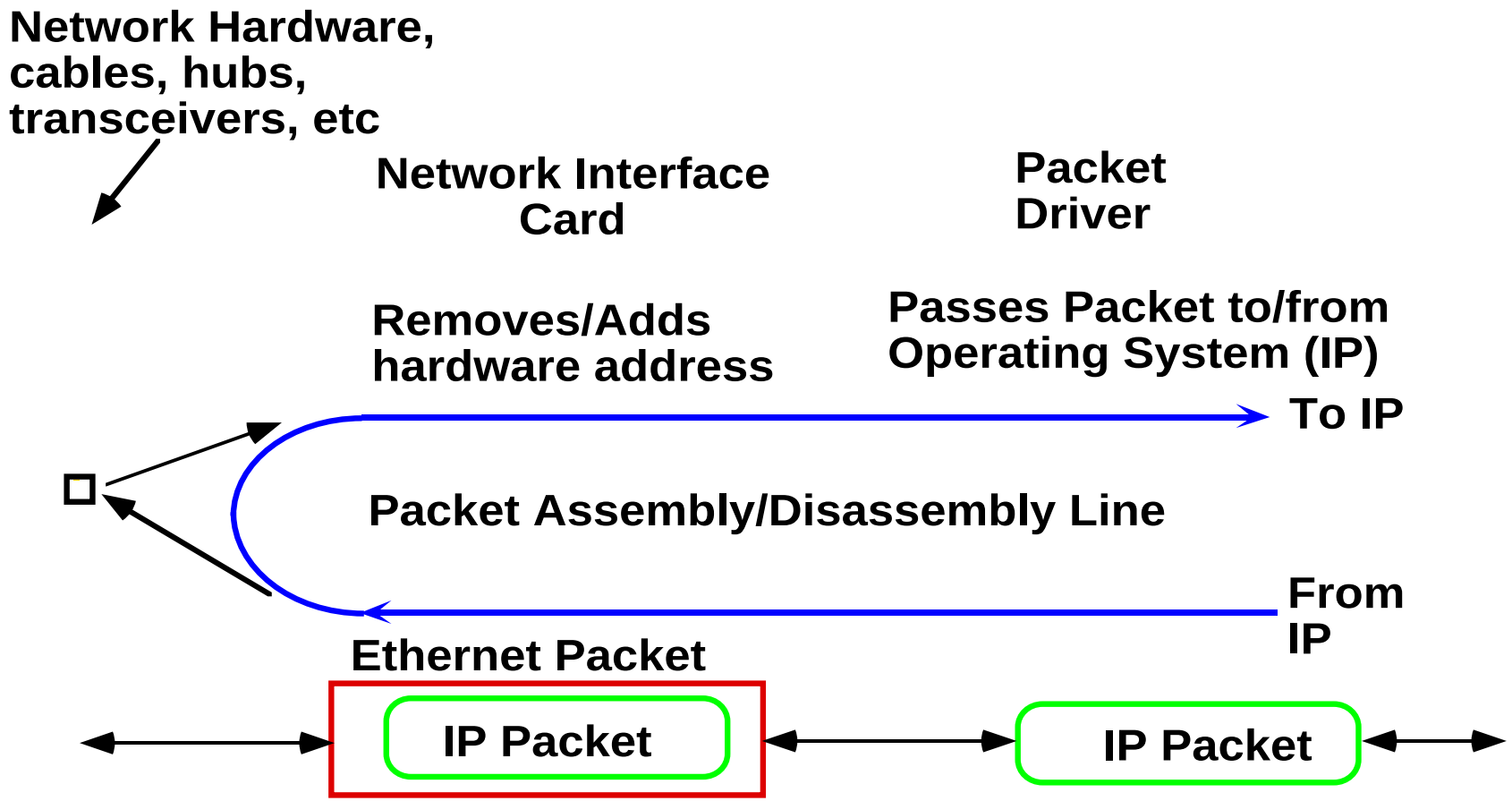
Used by Application layer protocols such as Name Server, Trivial File Transfer Protocol (TFTP), Remote Procedure Call (RPC), NFS and etc.

IP is used to deliver UDP packets

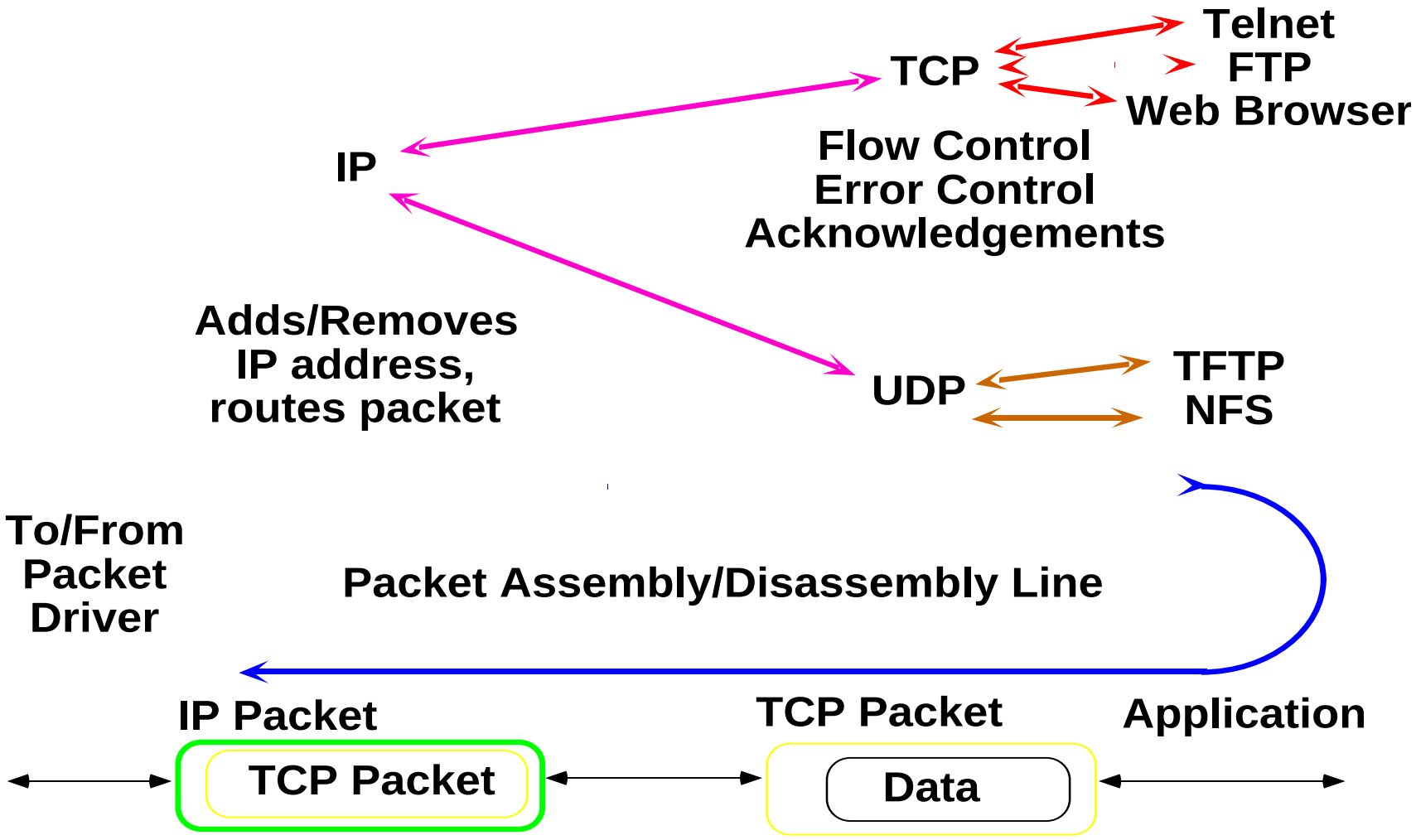
Unreliable, connectionless Datagram Services

More efficient than TCP and other Transport layer protocols, since no error detection

Packet Assembly/Disassembly Showing Hardware Portion



Packet Assembly/Disassembly Showing TCP/IP Portion



Application Layer Protocols

- **File Transfer Protocol (FTP)**

  - Resides at the top of TCP/IP
  - Invokes services from TCP
  - Provides services to the user
  - Services include connection establishing, file transfer

- **Telnet**

  - Like FTP, it uses TCP for providing services to users
  - Services include remote terminal sessions, terminal-to-processor and terminal to terminal communication

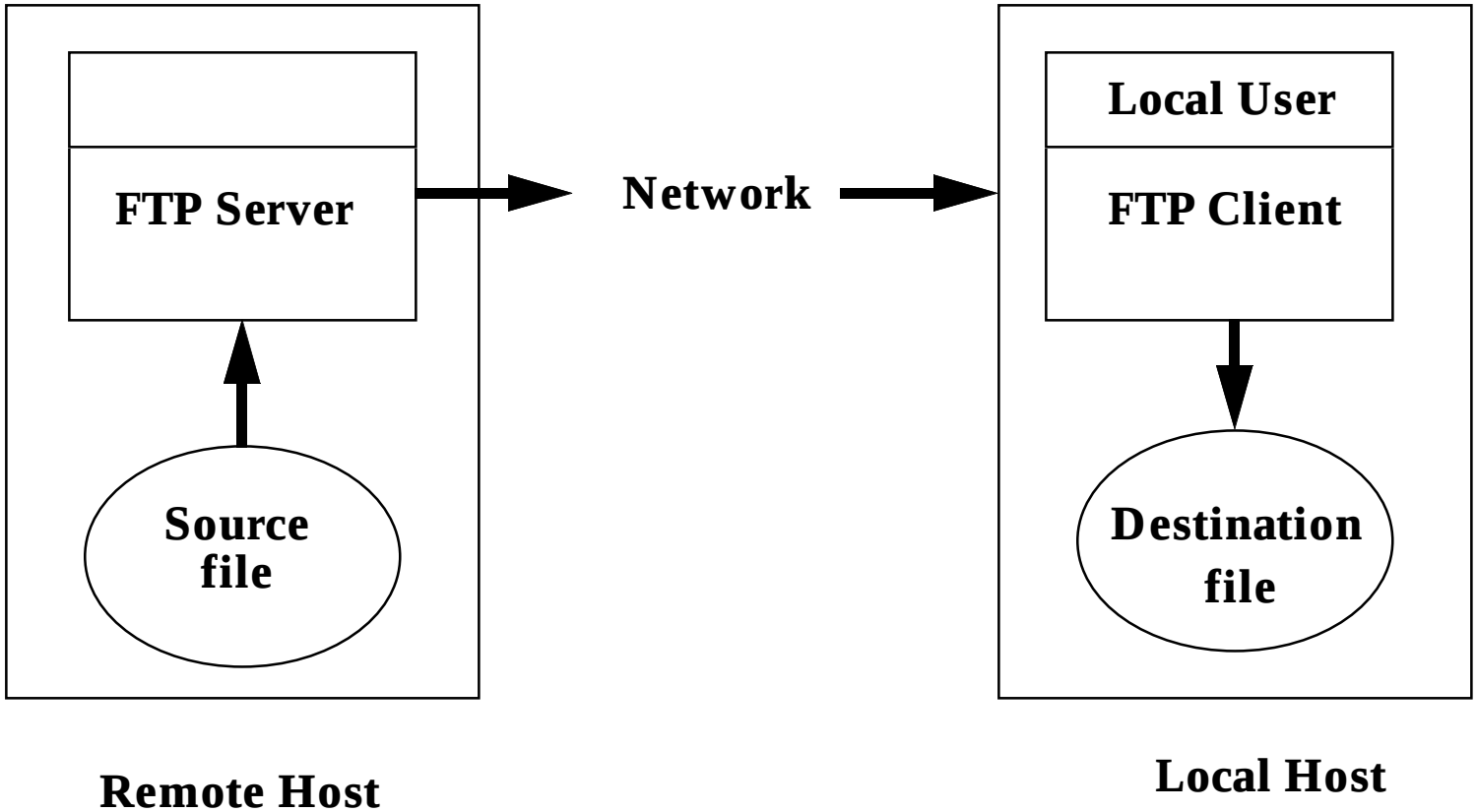
- **Simple Mail Transfer Protocol (SMTP)**

  - Sends and receives electronic mail

- **Simple Network Management Protocol (SNMP)**

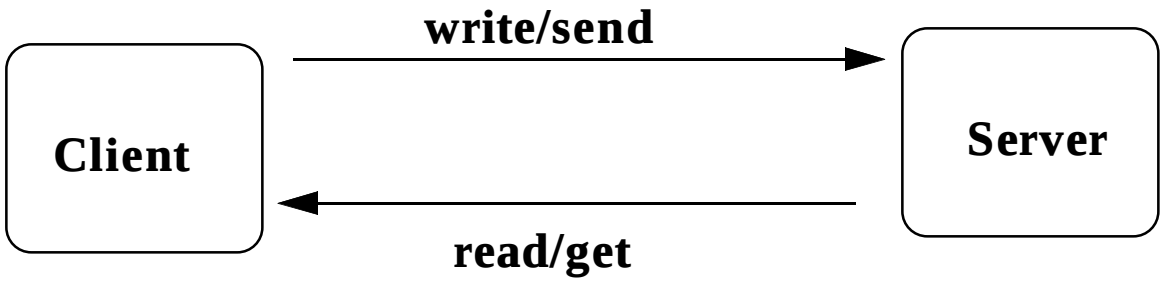
  - Performs management functions

File Transfer Transfer Protocol



File Transfer Protocol

- Three Issues
  - Data types - ASCII, EBCDIC, Bitstream, logical bytes
  - File Structure - Mac, PC, Unix.
  - Transmission Modes - Text (ASCII), Binary
- Client-Server mode of Operation

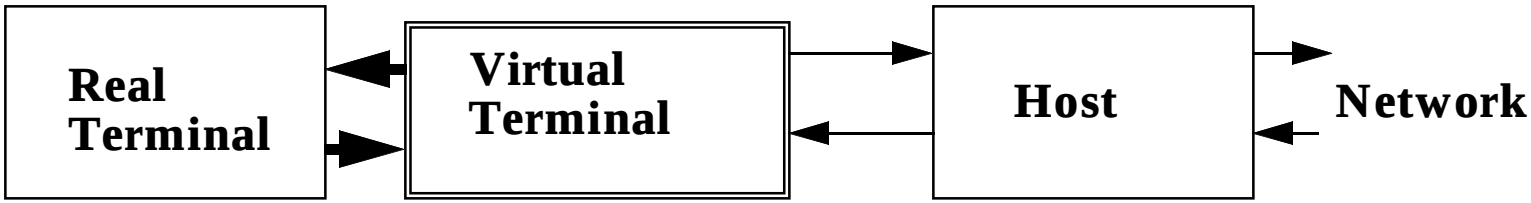


Telnet

- Provides a general bi-directional character-oriented (non-graphic) login facility between a local machine and a remote host, eg a super computer

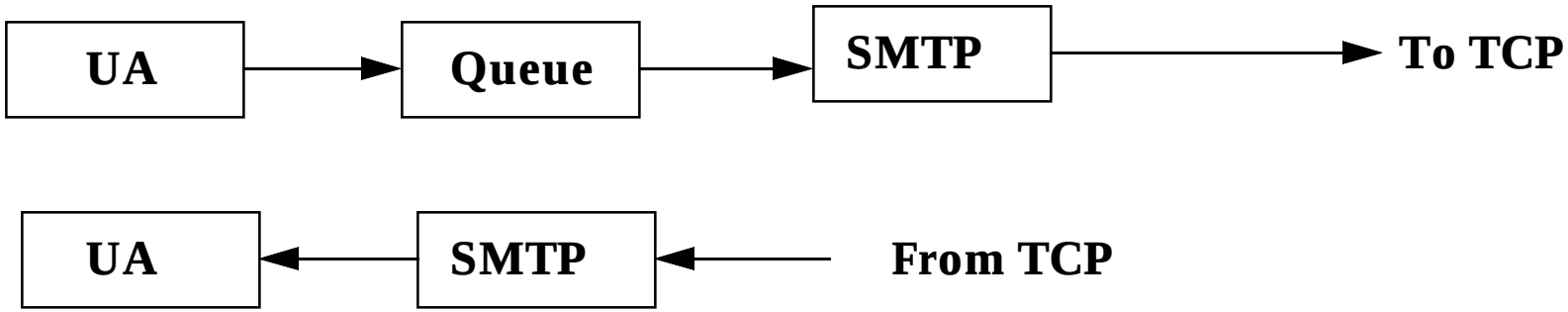
- Supports a number of systems through Network Virtual terminal (NVT)

- Has two parts - the User Telnet and the Server Telnet



Simple Mail Transfer Protocol

- Transfers mail between hosts using sender and receiver part

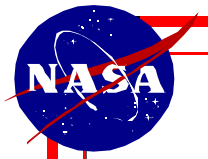


- **Sender** part needs two parts

  - The message text
  - A list of mail destinations

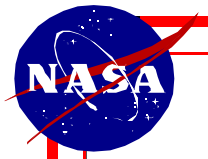
- **Mailbox specifications**

  user@localnet.network.zone



Section 4:

Network Management Using TCP/IP.

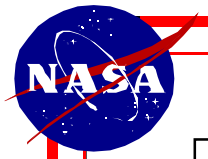


Network Management

- Previously, management was done on the hardware level, so developing a standard was a problem
- TCP/IP makes management an application level problem
- Internet gateways are used for storing management data
- Advantages
  - Independence from hardware and particular vendors
  - Uniformity - all gateways respond to same set of queries
  - Using TCP/IP gateways can be controlled either centrally or in a distributed way
- Disadvantages
  - If any of the TCP, IP or the OS goes down, gateways cannot be controlled

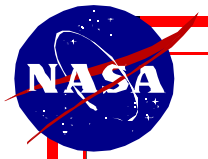
Functional Areas of Management

- **Configuration Management - physical and logical configuration**
- **Fault Management - uptime, down time**
- **Performance Management - delay , throughput**
- **Security Management - who can access the resources**
- **Accounting Management - how and by whom the network used**



Managing TCP/IP Networks

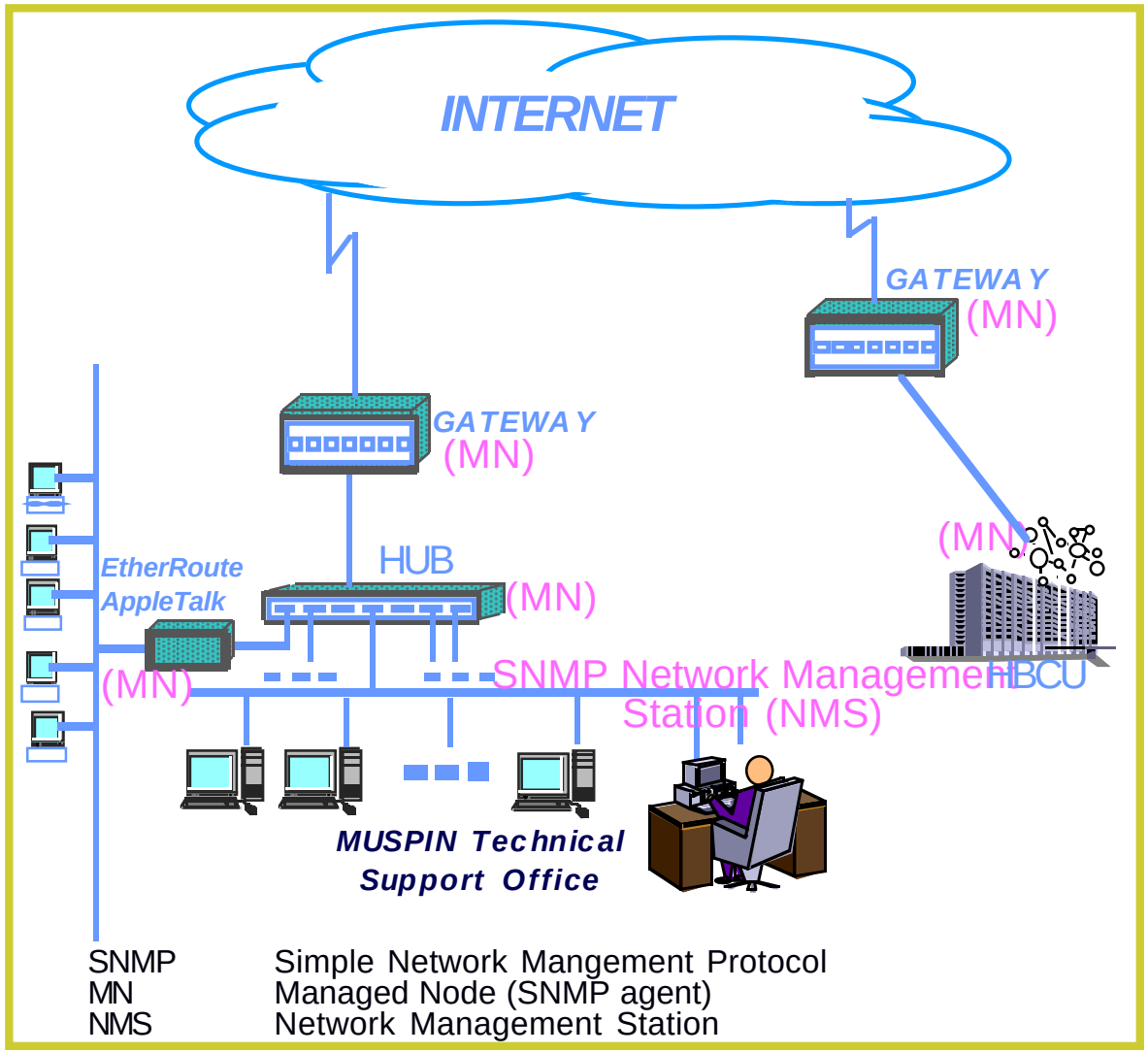
- A Client-Server mode of operation assumed
- A gateway runs the server software
- Controlling host runs the client software
- Authentication mechanism is required for accessing the server
- A management information base (MIB) keeps status report



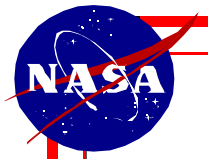
SNMP

- **Get-fetch paradigm**
- **Two commands - one to fetch a value from a data item and the other to store a value into a data item.**
- **Commands**
  - get-request - fetch a value
  - get-next-request - fetch value without a name
  - get-response - reply to a fetch operation
  - set-request - store value in a specific variable
  - trap - reply triggered by an event
- **The user interface can be designed to have imperatives for example, a program "reboot" can be written to set the time for next reboot equal to zero.**
- **The protocol is simple, stable and flexible**

SNMP Management



SNMP	Simple Network Mangement Protocol
MN	Managed Node (SNMP agent)
NMS	Network Management Station



Section 5:

Serial Line (Dial Up)

TCP/IP–SLIP and PPP

Point to Point Protocol - PPP

- PPP has the ability to allow to simultaneous use of multiple network-layer protocols over serial links
- PPP provides error detection and enhanced provisions for dealing with security
- PPP specifies the use of asynchronous or synchronous duplex circuits, either dedicated or circuit switched
- No login script needed - includes password authentication protocol
- Preferred method of dial up access
- Included with Trumpet Winsock

Serial Line IP - (SLIP)

- Device Driver that allows TCP/IP through serial port
- Allows computers to be connected remotely over asynchronous modem lines as if they were locally connected
- Available for IBM compatibles, Apple Macintosh and most Berkley UNIX-systems. It is included in the standard 4.3BSD release from Berkley
- SLIP is free via anonymous FTP over the Internet
- Included with Trumpet Winsock

PPP/SLIP Dial Up to the Internet